UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/814,337	03/21/2001	William J. Bolosky	MS1-735US	3684

22971 7590 02/28/2008

MICROSOFT CORPORATION
ONE MICROSOFT WAY
REDMOND, WA 98052-6399

EXAMINER	
GYORFI, THOMAS A	

ART UNIT	PAPER NUMBER
2135	

NOTIFICATION DATE	DELIVERY MODE
02/28/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

roks@microsoft.com
ntovar@microsoft.com
a-rydore@microsoft.com

Office Action Summary	Application No.	Applicant(s)	
	09/814,337	BOLOSKY ET AL.	
	Examiner	Art Unit	
	Thomas Gyorfi	2135	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *25 January 2008*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *9-11 and 13-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *9-11 and 13-22* is/are rejected.

7)☒ Claim(s) *21 and 22* is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____ .
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

DETAILED ACTION

1. Claims 9-11 and 13-22 remain for examination. The correspondence filed 1/25/08 amended claims 19, 21, and 22.

Claim Objections

2. It is observed that claims 21 and 22 are identified as being "new" claims (presumably in response to the claim objections from the Office Action of 10/29/07, page 2, paragraph #5), despite the fact that the claims were previously listed [with erroneous status] in the amendment of 8/7/07. For the sake of expediting prosecution of the case, Examiner hereby declares that the proper status of the claims was "New" as of 8/7/07, and "Currently Amended"[1] as of 1/25/08.

Response to Arguments

3. Applicant's arguments filed 1/25/08 have been fully considered but they are not persuasive. With respect to claims 9-11 & 13, Applicant argues that the combination of Howard and Freenet fail to teach “computing a hash value of the group” and “digitally signing the hash value of the group of hash values” (see page 8 of the amendment, first two paragraphs); Examiner respectfully disagrees. First, it is observed that the Howard system produces a single file – a journal file – whose content comprises a group of hash values representing other modified files in the distributed file system (col. 3, lines 25-40; cf. Figures 1 and 2). This journal file constitutes a “group of hash values” under the

[1] Both claims replaced the word “comprise” with the more grammatically correct “comprises”.

broadest reasonable definition of the term; additionally, Howard discloses wherein the journal file is stored in the distributed file system just like the user files it tracks (col. 4, lines 25-45). In that vein, the Freenet reference discloses wherein, when *any* file ***irrespective of its contents*** is to be stored in a distributed file system, said any file is hashed and digitally signed (pages 9-10, "5. Naming, searching, and updating"). If one were to apply these well-known distributed file system techniques to the distributed file system of the Howard invention, then the application of those techniques specifically on the journal file would logically result in the hash value of the group of hashes being computed and subsequently being digitally signed, just as disclosed in the claims.

4. Further regarding claim 9, in response to Applicant's argument that the instant invention employs encryption in a different capacity than does the Freenet system (page 9 of the amendment), the fact that Applicant has recognized another advantage which would flow naturally from following the suggestion of the prior art cannot be the basis for patentability when the differences would otherwise be obvious. See *Ex parte Obiaya*, 227 USPQ 58, 60 (Bd. Pat. App. & Inter. 1985). It is observed that the only recited limitation in the claim is that the distributed file system stores encrypted files, with the modified files being themselves encrypted; at no point in the claim is there any recitation for the encryption to secure a file or to deny a user access to a file as appears to be argued by the Applicant. Just because the instant invention might have a different reason for employing encryption than Freenet does, this does not obviate the fact that Freenet teaches an encrypting distributed file system exactly as recited by the claim(s). In traversing the rejection Applicant even quoted the pertinent passage of Freenet that

teaches in part that "...it is recommended that **all** inserted files be encrypted..." [emphasis Examiner's]; which establishes not only that Freenet teaches the claimed limitation of a distributed file system that encrypts files, but also that as a logical consequence of this preferred embodiment wherein all files in the system are encrypted, that any file to be modified or updated in a Freenet system must be an encrypted file.

5. With regards to claims 14-16, Examiner rebuts Applicant's arguments for substantially similar reasons as discussed above for claims 9-11 and 13.

6. With regards to claims 17, 18, & 22, Examiner again reminds Applicant that the journal file produced by the Howard invention qualifies as being "a representation of a collection of the representations of modifications", the individual "representations of modifications" being the individual entries in the journal file (Howard, Ibid). And as has been argued above, this journal file – by virtue of being a file itself – would also need to be stored in the distributed file system (see col. 4, lines 25-45). Similarly, Freenet discloses wherein any file to be stored in a distributed file system ***irrespective of its contents*** should be digitally signed first (Freenet, page 10, first paragraph). Additionally, Applicant's argument that "Freenet fails to make any mention of a digital signature **to indicate that modifications were made by a user with the signature**" (page 13 of the amendment, 1st paragraph) fails to take into account that this limitation is implicit in the use of a public/private key pair to perform digital signing, not just in the general case but also specifically as employed by Freenet. Referring again to the cited passage on page 10 of the Freenet disclosure, when a user wishes to modify a file in the distributed file system, the user creates a public/private key pair *indicative of the*

user and uses the private key to create the digital signature that represents the modified file. Anyone who wishes to verify the validity of the signature must use the corresponding public key (the "*signature-verifying key*", as per the parlance of Freenet) to do so. Given that anything encrypted by one key in a public/private key pair can only be decrypted by the other key, and given that the private key of the user who made the modification is held and known solely by said user, thus it stands to reason that if the signature is decrypted successfully using said user's public key, then one knows that the new version/modification was made by said user as only said user could have used the private key to create the signature in the first place. For Applicant's edification regarding the use of public/private key encryption in digital signatures, please consult the FIPS-186 reference cited by the Examiner in the Office Action of 10/20/05.

7. With regards to claims 19-21, Examiner rebuts Applicant's arguments for substantially similar reasons as discussed above for claims 17, 18, & 22.

8. In response to Applicant's various arguments regarding the motivation(s) previously cited by the Examiner to combine the Howard and Freenet references, it is noted that the teaching-suggestion-motivation test is no longer the sole means to establish obviousness of claimed subject matter, as has since been decided by the Supreme Court in *KSR v. Teleflex*, 550 U.S. at ___, 82 USPQ2d at 1395-1397. Accordingly, the rationale for the rejections herein has been rewritten to adhere to the guidelines set therein, rendering Applicant's arguments regarding motivation moot.

Claim Rejections - 35 USC § 103

9. The text of those sections of Title 35, U.S. Code not included in this action can be found in a prior Office action.

10. Claims 9-11 and 13-22 are rejected under 35 U.S.C. 103(a) as being unpatentable over Howard (U.S. Patent 6,098,079) and further in view of "Freenet: A Distributed Anonymous Information Storage and Retrieval System" (a.k.a. "Freenet").

Regarding claims 9 and 13:

Howard discloses a method and computer readable medium for use in a distributed file system comprising: modifying one or more of the files (col. 3, lines 25-30); computing a hash value of each modified file (col. 3, lines 30-40); and collecting the hash values into a group (the journal file: Ibid).

Howard does not explicitly disclose wherein the files are encrypted, nor that once the group of hash values has been collected, a hash value of the group is computed and digitally signed. However, it observed that the journal file – the group of hash values – maintained by Howard is itself a file as well (col. 3, lines 25-30) that is also stored in the distributed file system alongside the files it tracks (e.g. col. 4, lines 25-45). Furthermore, Freenet discloses an analogous distributed file system wherein all files irrespective of their content are hashed and then digitally signed (pages 9-10, "5. Naming, searching, and updating"). Freenet also teaches that it is preferable for all files on said distributed file system to be encrypted (page 7, "3.3 Managing Data", last paragraph). The claim is thus obvious because the respective techniques of hashing

and digitally signing files on Howard's distributed file system [including the journal file comprising a collection of hash values into a group], as well as performing operations on encrypted files, were all recognized as part of the ordinary capabilities of one of ordinary skill in the art, in view of the teaching of these techniques for improvement of similar distributed file systems such as that disclosed by Freenet.

Regarding claim 14:

Howard discloses a computer readable medium causing a computing device to: modify individual files stored in a serverless distributed file system (col. 3, lines 25-30); compute a hash value of each modified file (col. 3, lines 30-40); and collect the hash values into a group (the journal file: Ibid).

Howard does not disclose digitally signing the group of hash values. However, it observed that the journal file – the group of hash values – maintained by Howard is itself a file as well (col. 3, lines 25-30) that is also stored in the distributed file system alongside the files it tracks (e.g. col. 4, lines 25-45). Furthermore, Freenet discloses an analogous serverless distributed file system wherein all files irrespective of their content are digitally signed (pages 9-10, "5. Naming, searching, and updating", particularly the first paragraph of page 10). It would have been obvious to digitally sign the journal file of the Howard invention, because the technique of digitally signing *any* file stored in a serverless distributed file system as disclosed by Freenet was recognized as part of the ordinary capabilities of one skilled in the art, in view of the teaching of this technique being a known improvement to a similar serverless distributed file system.

Regarding claims 17 and 19:

Howard discloses a method (and computer readable medium) comprising: storing representations of modifications made to multiple files stored in a distributed file system such that each modification has a corresponding said representation (col. 4, lines 25-60); and a representation of a collection of the representations of modifications (the journal file, Figure 3; col. 4, lines 45-60).

Howard does not explicitly recite a digital signature covering at least part of the representations to indicate that the modifications were made by a user with the signature. However, Freenet discloses an analogous distributed file system wherein a user creates a digital signature covering at least part of the representations of an updated file(s) to indicate that the modifications were made by said user (pages 9-10, "5. Naming, searching, and updating", particularly the first paragraph on page 10). The claim is thus obvious because the technique of using a digital signature to verify that modifications were made by a particular user was recognized as part of the ordinary capabilities of one of ordinary skill in the art, in view of this technique being a known improvement to a related distributed file system. With respect to claim 19, as noted by Howard the journal file must itself be stored in the distributed file system (e.g. col. 4, lines 25-35); thus the use of a single digital signature to authenticate the journal file would also necessarily authenticate the contents of said journal file, i.e. the file authentication info for each of the multiple files (the individual hashes: Howard, col. 3, lines 25-30, and Figures 1 and 2).

Regarding claims 10 and 15:

Howard further discloses wherein the modified [encrypted] file includes a metadata stream containing a header and an indexing structure, the indexing structure including hashes of the files, and a structure to access the hashes of files, the computing a hash value of each modified file further comprising deriving a hash of the header and at least part of the structure (Figures 3-6; col. 5, lines 1-60)

Regarding claims 11 and 16:

Howard further discloses wherein the modified [encrypted] file includes a metadata stream containing a header, per user information, and an indexing tree, the indexing tree including hashes of files, and a root node, the computing a hash value of each modified file further comprising hashing as a single the header, the per user information, and the root node (Ibid).

Regarding claims 18 and 20:

Howard further discloses wherein the representations comprise hashes of data in each file that is affected by the modifications (Figure 5; col. 5, lines 15-20).

Regarding claims 21 and 22:

Freenet further discloses wherein the representation of the collection comprises a hash of the representations of the modifications (page 9, "5. Naming, searching, and updating", 2nd paragraph).

Claim Rejections - 35 USC § 101

11. Claims 9-11 and 13-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 13-18 and 22 recite "one or more computer readable media", which is explicitly defined in the specification on page 17, lines 14-18 as either or both of "computer storage media" (comprising various well known articles of manufacture, as per page 17, line 19 - page 18, line 2) and "communications media" (comprising various signal and ethereal embodiments, as per page 18, lines 3-12). The latter "communication media" forms of "computer readable media" have not been recognized by the courts as conforming to any of the statutory classes of invention; therefore the claims encompass non-statutory subject matter and are thus non-statutory. Examiner suggests that this rejection may be overcome for claims 13-18 and 22 by amending the claims to recite a "computer storage media" rather than "computer readable media", so as to limit the scope of the claims strictly to statutory embodiments; and, in addition, to amend the specification to remove the "communications media" as an embodiment of the instant invention for which patent protection is being sought..

Claims 9-11 are rejected as evidenced by claims 13-16; similarly, claims 19-21 are rejected as evidenced by claims 17, 18, and 22.

Conclusion

12. Any inquiry concerning this communication or earlier communications from the examiner should be directed to Thomas Gyorfi whose telephone number is (571)272-3849. The examiner can normally be reached on 8:30am - 5:00pm Monday - Friday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Kim Vu can be reached on (571) 272-3859. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only.For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/Thanhnga B. Truong/
Primary Examiner, Art Unit 2135

TAG
2/20/08